Office of the New York State Comptroller
Thomas P. DiNapoli, State Comptroller
Division of Local Government and School Accountability

LOCAL GOVERNMENT MANAGEMENT GUIDE

Information Technology Contingency Planning

For additional copies of this report contact:

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th floor
Albany, New York 12236
Tel: (518) 474- 4037
Fax: (518) 486- 6479
or email us: localgov@osc.state.ny.us

www.osc.state.ny.us

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller

October 2015

Table of Contents

Information technology (IT) has become an integral part of most local governments' and school districts' operations. Computer systems and electronic data are fundamental to daily business transactions, communication, and accounting and reporting. The impact of an unplanned IT disruption involving the corruption or loss of data or other computer resources from human error, malware or hardware failure, for example, could significantly curtail an organization's operations.

Proactively anticipating and planning for IT disruptions will prepare local government and school district personnel for the actions they must take in the event of an incident. The goal of IT contingency planning is to enable a computer system and/or electronic data to be recovered as quickly and effectively as possible following an unplanned disruption. The time to think about and plan for IT emergencies is before they occur.

The goal of IT contingency planning is to enable a computer system and/or electronic data to be recovered as quickly and effectively as possible following an unplanned disruption.

IT Contingency Planning

In general, a business continuity plan focuses on strategies for sustaining an organization's critical business processes in the event of a disruption. It provides detailed guidance for continuing operations as normally as possible during and after a major, unplanned incident. Since information technology often supports key business processes, planning specifically for IT disruptions is a necessary part of business continuity planning.

IT contingency planning refers to the plans, policies, procedures and technical measures that enable the recovery of IT operations after an unexpected incident. A disruptive event could include a major natural disaster such as a flood, or something smaller, such as malfunctioning software caused by a computer virus. Since no computer system can be expected to operate perfectly at all times, unplanned service interruptions are inevitable.

The content, length and resources necessary to prepare an IT contingency plan will vary depending on the size and sophistication of your organization's computerized operations. Larger organizations may need a suite of plans that go by many different names – business continuity, IT contingency, emergency management, incident response – to fully meet their planning needs.

In the event of an incident, personnel need to quickly recognize situations that are of greater severity and demand immediate attention.

Best Practices:

There are several steps entities can take to improve their chances of quickly recovering from an IT disruption.

Assemble a Team – Assemble a team responsible for drafting an IT contingency plan for management's review and approval. The team should include individuals with knowledge about critical business functions as well as those with appropriate technical knowledge of the organization's IT systems and electronic data. It may be necessary to include outside parties such as the organization's IT vendor, if applicable.

Identify Critical Processes and Services – Identify and prioritize the organization's critical business processes and services, and the IT systems, components and data that support the processes and services. In the event of an incident, personnel need to quickly recognize situations that are of greater severity and demand immediate attention. For example, if the payroll process is identified as a critical function, the plan should include an explanation of how payroll processing will continue in the event of an unplanned IT incident that renders the current payroll system inoperable and/or electronic data inaccessible.

Develop a Plan – Organizations should develop a written IT contingency plan that addresses the range of threats to their IT system(s), distribute the plan to all responsible parties, and ensure that it is periodically tested and updated as needed. The plan should focus on sustaining critical IT functions during and after a disruption. Technology recovery strategies should consider the possible restoration of hardware, applications, data and connectivity. The plan should also include policies and procedures to ensure that all critical information is routinely backed up so that it would be available in the event of an emergency.

An IT contingency plan is the organization's recovery strategy. It can include, among other items deemed necessary by the organization, the following:

- Roles and responsibilities of key personnel;
- Communication protocols with outside parties (e.g., law enforcement, IT vendors);
- Prioritized mission-critical processes and services;
- Technical details concerning how systems and data will be restored;
- Resource requirements necessary to implement the plan;
- Backup methods and storage policies (see next section entitled Backup Procedures); and
- Details concerning how the plan will be periodically tested.

The plan should also address how employees will communicate, where they will go and how they will continue to do their jobs during a disruption. The details will vary depending on the size and scope of the entity and its computerized operations. It's important to remember to distribute the plan and subsequent updates to all parties who have responsibilities in the event of a disruption; otherwise, the plan's value is significantly diminished.

Train Personnel and Test the Plan – Personnel expected to execute the plan must understand the plan and, as necessary, be trained to perform their duties. Where appropriate, elements of the plan should be tested. For example, by verifying the organization's ability to restore backup data. Subsequent revisions to the plan should be redistributed to key personnel to ensure they understand the changes.

Revise the Plan – The IT contingency plan should be periodically reviewed and, as appropriate, revised to ensure it still meets the organization's needs. Things such as changes in personnel, IT infrastructure, organizational priorities, or facilities identified as alternative processing sites may require plan revisions. The revised plan should then be distributed to personnel who have key responsibilities.

The IT contingency plan should be periodically reviewed and, as appropriate, revised to ensure it still meets the organization's needs.

Backup Procedures

While many organizations perform some type of backup procedure(s), far fewer periodically attempt to restore a backup to ensure the process is functioning as intended and that data would be available in the event of an emergency.

A backup is a copy of electronic information that is maintained for use if there is loss or damage to the original. Establishing backup procedures is a necessary part of IT contingency planning and often critical for restoring operations quickly and effectively following a service disruption.

Best Practices:

There are several steps entities can take to improve their ability to quickly restore electronic data.

Adopt a Data Backup Policy – Organizations should have a written policy describing their backup procedures. It should include the frequency and scope of backups, the location of stored backup data, the specific method for backing up and any other important details relating to the process (e.g., file-naming conventions, method of transporting data offsite). The policy should also address how the organization will periodically verify that the data has been backed up and how it will test its ability to restore backup data.

Back Up Data at Regular Intervals – The frequency (e.g., daily, weekly) and scope of backups (e.g., incremental or full) will be based on various factors such as the volume and frequency at which new electronic information enters the computer system and the criticality of the data.

Verifying Data Has Been Backed Up and Can Be Restored – While many organizations perform some type of backup procedure(s), far fewer periodically attempt to restore a backup to ensure the process is functioning as intended and that data would be available in the event of an emergency.

Store Backups in Offsite Location – Backups should be secured in an offsite location that meets the organization's data security requirements and other conditions of storage (e.g., temperature control, fire prevention). It is important to maintain offline copies of backups in case a cyberattack renders online files unusable. Some organizations contract with a third party for backing up data, application and/or operating system. If that is the case, the organization should have a written agreement with the vendor that clearly describes the expectations for safeguarding the data, especially if it contains personal, private and/or sensitive information (e.g., names and Social Security numbers). In addition, local governments should check with New York State Archives personnel to gain an understanding of the laws and regulations pertaining to offsite data storage. NYS Archives has issued a Records Advisory entitled Using a Data Storage Vendor[1] that describes what should be included in a data storage contract.

[1] **http://www.archives.nysed.gov/records/mr_data_storage.shtml**.

Additional Resources

Multi-State Information Sharing & Analysis Center (MS-ISAC)
http://msisac.cisecurity.org/

National Institute of Standards and Technology (NIST), Computer Security Division
http://csrc.nist.gov/publications/PubsSPs.html

New York State Office of Information Technology Services
https://www.its.ny.gov/local-government

United States Computer Emergency Readiness Team (US-CERT)
https://www.us-cert.gov/

Division of Local Government and School Accountability

Central Office Directory

Andrew A. SanFilippo, Executive Deputy Comptroller

(Area code for the following is 518 unless otherwise specified)

Executive 474-4037
Gabriel F. Deyo, Deputy Comptroller

Audits, Local Government Services and Professional Standards 474-5404
(Audits, Technical Assistance, Accounting and Audit Standards)

Local Government and School Accountability Help Line ..... (866) 321-8503 or 408-4934
(Electronic Filing, Financial Reporting, Justice Courts, Training)

New York State & Local Retirement System

Retirement Information Services

Inquiries on Employee Benefits and Programs 474-7736

Bureau of Member and Employer Services ..... (866) 805-0990 or 474-1101

Monthly Reporting Inquiries 474-1080

Audits and Plan Changes 474-0167

All Other Employer Inquiries 474-6535

Division of Legal Services

Municipal Law Section 474-5586

Other OSC Offices

Bureau of State Expenditures 486-3017

Bureau of State Contracts 474-4622

Mailing Address for all of the above:

Office of the New York State Comptroller,
110 State Street, Albany, New York 12236
email: **localgov@osc.state.ny.us**

Division of Local Government and School Accountability

Regional Office Directory

Andrew A. SanFilippo, Executive Deputy Comptroller

Gabriel F. Deyo, Deputy Comptroller (518) 474-4037

Cole H. Hickland, Director • **Jack Dougherty**, Director
Direct Services (518) 474-5480

BINGHAMTON REGIONAL OFFICE - H. Todd Eames, Chief Examiner
State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417
Tel (607) 721-8306 • **Fax** (607) 721-8313 • **Email:** Muni-Binghamton@osc.state.ny.us
Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins counties

BUFFALO REGIONAL OFFICE – Jeffrey D. Mazula, Chief Examiner
295 Main Street, Suite 1032 • Buffalo, New York 14203-2510
Tel (716) 847-3647 • **Fax** (716) 847-3643 • **Email:** Muni-Buffalo@osc.state.ny.us
Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming counties

GLENS FALLS REGIONAL OFFICE - Jeffrey P. Leonard, Chief Examiner
One Broad Street Plaza • Glens Falls, New York 12801-4396
Tel (518) 793-0057 • **Fax** (518) 793-5797 • **Email:** Muni-GlensFalls@osc.state.ny.us
Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington counties

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief Examiner
NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533
Tel (631) 952-6534 • **Fax** (631) 952-6530 • **Email:** Muni-Hauppauge@osc.state.ny.us
Serving: Nassau, Suffolk counties

NEWBURGH REGIONAL OFFICE – Tenneh Blamah, Chief Examiner
33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725
Tel (845) 567-0858 • **Fax** (845) 567-0080 • **Email:** Muni-Newburgh@osc.state.ny.us
Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester counties

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner
The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608
Tel (585) 454-2460 • **Fax** (585) 454-3545 • **Email:** Muni-Rochester@osc.state.ny.us
Serving: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief Examiner
State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428
Tel (315) 428-4192 • **Fax** (315) 426-2119 • **Email:** Muni-Syracuse@osc.state.ny.us
Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence counties

STATEWIDE AUDIT - Ann C. Singer, Chief Examiner
State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417
Tel (607) 721-8306 • **Fax** (607) 721-8313

Office of the New York State Comptroller • Thomas P. DiNapoli, State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor • Albany, New York 12236